

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平11-500241

(43) 公表日 平成11年(1999) 1月6日

(51) Int.Cl.⁹

G 0 9 C 1/00

識別記号

6 5 0

F I

G 0 9 C 1/00

6 5 0 Z

6 5 0 B

審査請求 有 予備審査請求 有 (全 34 頁)

(21) 出願番号 特願平9-518885
(86) (22) 出願日 平成8年(1996)10月31日
(85) 翻訳文提出日 平成10年(1998)5月18日
(86) 国際出願番号 PCT/US 96/17449
(87) 国際公開番号 WO 97/18652
(87) 国際公開日 平成9年(1997)5月22日
(31) 優先権主張番号 08/559, 213
(32) 優先日 1995年11月16日
(33) 優先権主張国 米国 (US)
(81) 指定国 EP (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), CA, JP

(71) 出願人 ベル コミュニケーションズ リサーチ、
インコーポレイテッド
アメリカ合衆国 07960 ニュージャージー
州 モーリスタウン サウス ストリート 445
(72) 発明者 アイエロ, ウィリアム, エイ.
アメリカ合衆国 07940 ニュージャージー
州 マディソン メイプル アヴェニュー 54
(72) 発明者 ヴェンカテサン, ラマラスナン
アメリカ合衆国 07960 ニュージャージー
州 モーリスタウン コンクリン アヴェニュー 9
(74) 代理人 弁理士 谷 義一 (外3名)

(54) 【発明の名称】 ハッシュ関数および疑似ランダム関数の安全性を高める効率的な暗号ハッシュ関数および方法

(57) 【要約】

暗号ハッシュ関数回路 (300) はテーブル (301, 302, ..., 303) を有しており、テーブル (301, 302, ..., 303) への入力バス (311, 312, ..., 313) 上の入力 $c_i(j)$ を有し、出力バス (321, 322, ..., 323) 上への出力を作成して、排他的論理和ゲート (331) へ印加する。排他的論理和ゲートの出力は、バス (351) 上の k_i である。キー K は 8 個の k_i の連結である。

FIG. 3

